**Билет 21.**

**Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предотвращения. Интернет-мошенничество и способы защиты от него.**

Расширение областей использования компьютеров, высокая степень концентрации информации, расширение доступа пользователя к мировым информационным ресурсам, усложнение программного обеспечения привело к тому, что некоторые действия программистов, специалистов, работающих с информацией, обычных пользователей могут быть квалифицированы как **правонарушения** (преступления).

К видам компьютерных преступлений относят:

* несанкционированный доступ к информации, хранящейся в компьютере;
* ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;
* разработка и распространение компьютерных вирусов;
* хищение компьютерной информации.

Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

В законодательстве России имеются законы и акты, регулирующие вопросы информации и информатизации. В частности, Закон **«О правовой охране программ для ЭВМ и баз данных»**регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных. В нем дано юридическое определение таких понятий, как авторство, база данных, воспроизведение, декомпилирование, использование, модификация и т.д. При создании программ и баз данных принято различать авторские и имущественные права.

**Авторское право**распространяется на программы для компьютеров и базы данных, являющиеся результатом творческой деятельности автора. Однако авторское право не распространяется на идеи и принципы, лежащие в основе программ и базы данных, какого-либо их элемента, например на организацию интерфейса, т.е. внешнего вида программы.

**Имущественное право**на программы для компьютеров и базы данных, созданные в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю. Таким образом, имущественное право на программу, созданную в ходе дипломного проектирования, принадлежит не студенту, а учебному заведению.

Выпуск под своим именем чужой программы или базы данных, а также незаконное воспроизведение или распространение таких произведений влечет за собой уголовную ответственность.

Закон **«Об информации, информатизации и защите информации»**регулирует, в частности, отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* обеспечении защиты информации.

Согласно закону граждане обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

В **Уголовном кодексе Российской Федерации**имеется глава, посвященная преступлениям в сфере компьютерной информации. В частности, неправомерный доступ к компьютерной информации квалифицируется как преступление при следующих условиях:

* если компьютерная информация охраняется законом;
* если неправомерный доступ к компьютерной информации повлек ее уничтожение, блокирование, модификацию, копирование.

Также предусмотрена уголовная ответственность за создание, использование и распространение вредоносных программ. Под вредоносными программами понимают программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также приводящие к нарушению работы компьютеров.

**Меры противодействия компьютерным преступлениям**можно подразделить на технические, организационные и правовые.

К **техническим мерам**можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности.

К **организационным мерам**относятся охрана компьютерных систем, вычислительных центров, подбор квалифицированного персонала, исключение случаев ведения особо важных работ одним человеком, наличие плана восстановления работоспособности после выхода оборудования из строя.

К **правовым мерам** следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав, совершенствование уголовного и гражданского законодательства.

С ростом электронных расчетов и развитием технологий человек все больше сталкивается с киберпреступностью. Многие незаконно взламывают пароли, приобретают деньги. Отсюда следует знать, как можно защитить себя во Всемирной паутине.

Слово «мошенники» применимо уже не только для реального мира, но и для виртуального. Киберпреступники хотят получить доход и нажиться, все они совершают свои деяния продуманно. Еще до развития Глобальной сети основную электронную опасность представляли вирусы. Их создавало небольшое количество людей, и угроза не распространялась быстро. В настоящее время мошенники работают сформированными группами, пытающимися захватить как можно больше денег. Они создают специальные программы, которые отсылают пользователям Сети, а затем получают нужные данные или проводят электронные операции.

***Пути проникновения вирусов.***

Вредные программы попадают на компьютер из—за незащищенности операционной системы или посредством социальной инженерии. На деле уязвимость системы устраняют ее разработчики, поэтому неполадки исправляются с каждым обновлением. А вот социальная инженерия является эффективным способом проникновения вредоносной программы в компьютер. Человек, занимающийся социальной инженерией, создает технологии, влияющие на эмоции и поведение людей.

Примеры кибератак, что довольно часто встречаются в Интернете

* 1.**Электронные письма**

Пользователю могут приходить письма с прикрепленным файлом, который на самом деле вовсе не является документом. Если пользователь откроет файл, то активирует троянскую программу. Злоумышленники присылают письма под именем банка, поэтому человек неосознанно заражает свой компьютер.

* 2. **Фишинг**

Фишинг – это один из самых распространенных видов мошенничества. Суть его заключается в том, что киберпреступники создают сайты, которые своим дизайном и наполнением очень похожи на настоящие. Поэтому интернет—пользователь при введении своего логина и пароля лишь сообщает свои данными мошенникам. Сайт—подделку отличает лишь неправильно написанное название в адресной строке.

* 3. **Сайт и фишинговые письма**

В социальных сетях довольно часто встречаются сообщения с линком, на который нужно перейти, чтобы узнать детали. Часто такие ссылки отправляют пользователей на сайт злоумышленников, где требуется опять вводить логин и пароль от социальной сети, чтобы другие люди могли их получить.

* 4. **Вызов эмоций**

Нередко киберпреступники пытаются вызвать у людей эмоциональную реакцию. Они составляют заголовки или тексты писем таким образом, что человек сразу хочет открыть файл. Например, получив сообщение от друга с текстом «Посмотри, как ты превосходно получился на видео!», пользователь из любопытства нажимает на ссылку скачивания, тем самым пускает вредоносную программу на свой компьютер. Прочитав подобные сообщения, подумайте, почему не указаны конкретные подробности и что это за видео. Важно не торопиться переходить по ссылкам и открывать неизвестные материалы.

Таким образом, в настоящее время имеется множество видов мошенничества в Глобальной сети.

Стандартные способы защиты от киберпреступников:

* 1. **Надежный пароль**

Придумывайте пароли, которые сочетают в себе большие и маленькие буквы, цифры, прочие символы. Не применяйте один и тот же пароль для значимых сайтов, например, не стоит для кошелька веб—мани составлять такой же пароль, как и для почты**.**2. **Обновление системы и антивируса**

Следует обновлять систему или антивирус, как только станут доступны новые обновления. Это будет способствовать защите от недавних электронных угроз. Желательно иметь лицензионную версию антивируса и постоянно проверять компьютер.

* 3. **Привязка телефона**

На многих сервисах есть функция привязки номера мобильного телефона. Если кто—то будет заходить в чужую электронную почту с нового устройства, программа, помимо логина и пароля, потребует подтверждения из СМС—сообщения. Это в разы увеличивает шансы защиты своей информации.

* 4. **Внимательность и недоверие**

Необходимо очень осторожно и бдительно относиться к подозрительным письмам и ссылкам, лучше их сразу удалять. Никогда не вводите свой пароль от социальной сети на неизвестных сайтах.

# В РФ существуют существует Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ, который содержит 18 статей.

В России действуют законы, где описано, как правильно работать с информацией: кто отвечает за ее сохранность, как ее собирать, обрабатывать, хранить и распространять. Стоит знать их, чтобы случайно что-нибудь не нарушить.

Мы собрали для вас пять основных ФЗ о защите информации и информационной безопасности и кратко рассказали их ключевые моменты.

149-ФЗ «Об информации, информационных технологиях и о защите информации»

149-ФЗ — главный закон об информации в России. Он определяет ключевые термины, например, говорит, что информация — это любые данные, сведения и сообщения, представляемые в любой форме. Также там описано, что такое сайт, электронное сообщение и поисковая система. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

**Ключевые моменты закона об информационной безопасности:**

1. Нельзя собирать и распространять информацию о жизни человека без его согласия.
2. Все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.
3. Есть информация, к которой нельзя ограничивать доступ, например сведения о состоянии окружающей среды.
4. Некоторую информацию распространять запрещено, например ту, которая пропагандирует насилие или нетерпимость.
5. Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.
6. У государства есть [реестр запрещенных сайтов](https://eais.rkn.gov.ru/). Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.
7. Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор — тогда его сайт разблокируют.

152-ФЗ «О персональных данных»

Этот закон регулирует работу с персональными данными — личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников. Мы подробно рассматривали этот закон в отдельной статье «Как выполнить 152-ФЗ о защите персональных данных и что с вами будет, если его не соблюдать»

**Ключевые моменты закона:**

1. Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.
2. Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.
3. Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.
4. Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.
5. Если вы работаете с персональными данными, то обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе — жесткого запрета на трансграничную передачу данных нет.

Серверы облачной платформы VK Cloud Solutions (бывш. MCS) находятся на территории РФ и соответствуют всем требованиям 152-ФЗ. В публичном облаке VKможно хранить персональные данные в соответствии с УЗ-2, 3 и 4. Для хранения данных с УЗ-2 и УЗ-1 также есть возможность сертификации, как в формате частного облака, так и на изолированном выделенном гипервизоре в ЦОДе VK.

При построении гибридной инфраструктуры для хранения персональных данных на платформе VK Cloud Solutions (бывш. MCS) вы получаете облачную инфраструктуру, уже соответствующую всем требованиям законодательства. При этом частный контур нужно аттестовать, в этом могут помочь специалисты VK, что позволит быстрее пройти необходимые процедуры.

98-ФЗ «О коммерческой тайне»

Этот закон определяет, что такое коммерческая тайна, как ее охранять и что будет, если передать ее посторонним. В нем сказано, что коммерческой тайной считается информация, которая помогает компании увеличить доходы, избежать расходов или получить любую коммерческую выгоду.

**Ключевые моменты закона о защите информации компании:**

1. Обладатель информации сам решает, является она коммерческой тайной или нет. Для этого он составляет документ — перечень информации, составляющей коммерческую тайну.
2. Некоторые сведения нельзя причислять к коммерческой тайне, например, информацию об учредителе фирмы или численности работников.
3. Государство может затребовать у компании коммерческую тайну по веской причине, например, если есть подозрение, что компания нарушает закон. Компания обязана предоставить эту информацию.
4. Компания обязана защищать свою коммерческую тайну и вести учет лиц, которым доступна эта информация.
5. Если кто-то разглашает коммерческую тайну, его можно уволить, назначить штраф или привлечь к уголовной ответственности.

63-ФЗ «Об электронной подписи»

Этот закон касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать.

**Ключевые моменты закона:**

1. Для создания электронной подписи можно использовать любые программы и технические средства, которые обеспечивают надежность подписи. Вы не обязаны использовать для этого какое-то конкретное государственное ПО.
2. Подписи бывают простые, усиленные неквалифицированные и усиленные квалифицированные. У них разные технические особенности, разные сферы применения и разный юридический вес. Самые надежные — усиленные квалифицированные подписи, они полностью аналогичны физической подписи на документе.
3. Те, кто работает с квалифицированной подписью, обязаны держать в тайне ключ подписи.
4. Выдавать электронные подписи и сертификаты, подтверждающие их действительность, может только специальный удостоверяющий центр.

187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Этот закон касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан России.

К таким сферам относится здравоохранение, наука, транспорт, связь, энергетика, банки, топливная промышленность, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность и химическая промышленность. Также сюда относят компании, которые обеспечивают работу предприятий из этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них ПО.

Если на предприятии из этой сферы будет простой, это негативно отразится на жизни всего государства. Поэтому к IT-инфраструктуре и безопасности информационных систем на этих предприятиях предъявляют особые требования.

**Ключевые моменты закона об информационной безопасности критически важных структур:**

1. Для защиты критической инфраструктуры существует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
2. Объекты критически важной инфраструктуры обязаны подключиться к ГосСОПКА. Для этого нужно купить и установить специальное ПО, которое будет следить за безопасностью инфраструктуры компании.
3. Одна из мер предупреждения — проверка и сертификация оборудования, ПО и всей инфраструктуры, которая используется на критически важных предприятиях.
4. Субъекты критической информационной инфраструктуры обязаны сообщать об инцидентах в своих информационных системах и выполнять требования государственных служащих. Например, использовать только сертифицированное ПО.
5. Все IT-системы критически важных предприятий должны быть защищены от неправомерного доступа и непрерывно взаимодействовать с ГосСОПКА.
6. При разработке IT-инфраструктуры критически важные предприятия должны руководствоваться 239 приказом ФСТЭК. В нем прописаны основные требования к защите информации на таких предприятиях.
7. Государство имеет право проверять объекты критически важной инфраструктуры, в том числе внепланово, например, после компьютерных инцидентов вроде взлома или потери информации.